Trials@uspto.gov
Tel: 571-272-7822

Paper 43
Entered: August 30, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00812
Patent 8,850,009 B2

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges.*

BISK, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a)

INTRODUCTION

A. *Background*

Petitioner, Apple Inc., filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–8, 10–20, and 22–25 (the "challenged claims") of U.S. Patent No. 8,850,009 B2 (Ex. 1003, "the '009 patent"). Patent Owner, VirnetX Inc., filed a Preliminary Response. Paper 6 ("Prelim. Resp."). We granted the Petition, instituting trial on whether claims 1–8, 10–20, and 22–25 are unpatentable as obvious over Beser[1] and RFC 2401.[2] Paper 8 ("Inst. Dec.").

During the trial, Patent Owner filed a Response (Paper 24, "PO Resp."), and Petitioner filed a Reply (Paper 28, "Reply"). Additionally, Patent Owner filed a Motion to Exclude evidence. Paper 35. A consolidated hearing for oral arguments in this *inter partes* review and Cases IPR2015-00810 and IPR2015-00811 was held June 8, 2016. A transcript of the hearing appears in the record. Paper 42 ("Tr.").

This is a Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons set forth below, Petitioner has shown by a preponderance of the evidence that claims 1–8, 10–20, and 22–25 are unpatentable.

---

[1] U.S. Patent No. 6,496,867 B1 (Ex. 1007) ("Beser").

[2] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998 (Ex. 1008) ("RFC 2401").

B. *The ’009 Patent*

The ’009 patent describes secure methods for communicating over the Internet. Ex. 1003, 10:16–17. Specifically, the ’009 patent describes “the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.” *Id.* at 39:36–38. This automatic process makes use of a modified Domain Name Server. In context, the ’009 patent describes a conventional Domain Name Server (DNS) as follows:

> Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name “Yahoo.com,” the user’s web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user’s browser and then used by the browser to contact the destination web site.

Id. at 39:39–45.

The modified DNS server may include both a conventional DNS and a DNS proxy. *Id.* at 40:33–35. The DNS proxy intercepts all DNS lookup requests, determines whether the user has requested access to a secure site (using, for example, a domain name extension or an internal table of secure sites) and if so, determines whether the user has sufficient security privileges to access the requested site. *Id.* at 40:39–45. If the user has requested access to a secure site to which it has insufficient security privileges, the DNS proxy returns a “host unknown” error to the user. *Id.* at 40:62–65. If the user has requested access to a secure site to which it has sufficient security privileges, the DNS proxy requests a gatekeeper create a VPN between the user’s computer and the secure target site. *Id.* at 40:45–51. The DNS proxy

then returns to the user the resolved address passed to it by the gatekeeper, which need not be the actual address of the destination computer. *Id.* at 40:51–57.

The VPN is "preferably implemented using the IP address 'hopping' features" (changing IP addresses based upon an agreed upon algorithm), described elsewhere in the '009 patent, "such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted." *Id.* at 40:18–22.

C. *The Challenged Claims*

Claims 1 and 14 of the challenged claims are independent and similar in scope. Claims 2–8 and 10–13 depend either directly or indirectly from claim 1 and claims 15–20 and 22–25 depend either directly or indirectly from claim 14. Claim 1 is illustrative of the claimed subject matter and recites:

1. A network device, comprising:

a storage device storing an application program for a secure communications service; and

at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:

send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device;

receive, following interception of the DNS request and a determination that the second network device is available for the secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of

> the second network device, and (3) provisioning information for an encrypted communication link;
>
> connect to the second network device over the encrypted communication link, using the received network address of the second network device and the provisioning information for the encrypted communication link; and
>
> communicate data with the second network device using the secure communications service via the encrypted communication link,
>
> the network device being a device at which a user uses the secure communications service to access the encrypted communication link.

Ex. 1003, 56:22–48.

CLAIM CONSTRUCTION

We interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). We presume a claim term carries its "ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question" at the time of the invention. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) (citation and quotations omitted). The Board construed claim terms similar to those at issue here in a proceeding challenging a patent related to the '009 patent. *Apple Inc. v. VirnetX Inc.*, IPR2014-00237 (PTAB May 11, 2015) (Paper No. 41) (final written decision "'237 FWD," or generally, "'237 IPR") (on appeal at the Federal Circuit); *see also VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1317–19 (Fed. Cir. 2014) (addressing ancestor *VirnetX* patents having similar claim terms).

A. *DNS Request*

The parties agree that the broadest reasonable interpretation of the term "DNS Request" is "a request for a resource corresponding to a domain name." Pet. 10; Prelim. Resp. 24; PO Resp. 3. We agree this is a reasonable construction and adopt this definition for purposes of this Decision.

B. *Interception of the DNS Request*

Petitioner proposes we construe the term "interception of a DNS request" as including "receiving a DNS request pertaining to a first entity at another entity." Pet. 10–11. In its Preliminary Response, Patent Owner argued that no construction was necessary for the term, but stated that if "the Board decides to provide a construction," the proper definition is "receiving a request to look up an internet protocol address and, apart from resolving it into an address, performing an evaluation on it related to establishing an encrypted communication link." Prelim. Resp. 25–28. Because the construction of this term was not dispositive to the Institution Decision, we did not expressly construe it at that time. Inst. Dec. 6.

In its Response, Patent Owner continues to assert that "[n]o construction is necessary" for the term "interception of the DNS request." PO Resp. 4. Patent Owner, however, also repeats its argument that if we do expressly construe this term, we should adopt the definition set forth in Patent Owner's Preliminary Response. *Id.* at 4–5 (incorporating by

reference arguments from the Preliminary Response Prelim. Resp. 25–28)[3] (citing Ex. 2016 ¶ 31).

In a related proceeding, we construed the similar phrase "intercepting a request" as "receiving a request pertaining to a first entity at another entity." '237 FWD 10–12. In this proceeding, as in the '237 IPR, we determine that this term requires construction to resolve an issue of patentability. For essentially the same reasons as those articulated in the '237 FWD, as explained below, we conclude that the term "interception of the DNS request" includes receiving a DNS request pertaining to a first entity at another entity.

Patent Owner argues that the claimed embodiments of the '009 patent "differ from conventional DNS, in part, because they apply an additional layer of functionality to a request to look up a network address beyond merely resolving it and returning the network address." Prelim. Resp. 27. According to Patent Owner, "Petitioner's construction overlooks the aspects distinguishing the 'intercepting' phrase from conventional DNS." *Id.* Instead, Patent Owner asserts that its proposed construction "appropriately captures" the additional functionality. *Id.* at 27–28; PO Resp. 4–5.

[3] It is necessary for the panel to refer to Patent Owner's arguments in the Preliminary Response in an effort to maintain a clear record. These arguments, however, are improperly incorporated by reference into Patent Owner's Response. *See* 37 C.F.R. § 42.6(a)(3); Paper 9, 2–3. Patent Owner is cautioned that by incorporating arguments by reference, it runs the risk that they are disregarded.

Patent Owner's arguments and the record, however, show that Patent Owner's proposed construction adds unnecessary functionality to "interception of a DNS request." According to Patent Owner's arguments, another recited phrase in claim 1 (and a similar phrase in claim 14), captures the functionality, in particular, the "determination" limitation of claim 1. *See* Prelim. Resp. 28 (listing one example function to be incorporated as "a determination is made that the request to look up the network address corresponds to a device that is available for the secure communications service" and "that 'following' this determination [limitation] 'provisioning information' required to initiate the encrypted communication link is provided"). In other words, the "determination" limitation already covers functionality that Patent Owner urges is implicit in the term at issue here. *See* Prelim. Resp. 27–28; PO Resp. 4–5.

The parties agree that "interception of a request" (at least) involves "receiving a request" at some device. PO Resp. 4; Pet. 10–11. Patent Owner's proposed construction, however, does not create any distinction between the receiving and intercepting of a request. According to Petitioner's proposed construction, an "interception" by the proxy DNS includes "receiving" a request to look up an address for another entity. In essence, Petitioner's construction captures the notion of interception as disclosed in the '009 patent, by requiring receiving to "pertain" to another entity. Patent Owner, however, can point to nothing in its proposed definition that captures the notion of interception. *See* Tr. 34:19–37:11.

Patent Owner alleges that Dr. Tamassia adopted an "intent" requirement in the "interception" clause—meaning a request must be

"intended for" or "ordinarily received by" another entity than that which ultimately intercepts it. PO Resp. 31–32 & n.4. Petitioner disagrees with any intent requirement, and contends that Patent Owner mischaracterizes Beser's disclosure. Reply 15–17.

Patent Owner addresses this "intent" requirement in an attempt to distinguish its claims over the prior art, and does not propose it as part of its claim construction. *See* PO Resp. 31–33; Tr. 31:1–34:18. And although Patent Owner points to language in the '237 IPR's institution decision using the "intended for" language ('237 IPR, Paper 15, 12), any alleged requirement of "intent" did not survive to the '237 FWD. *Compare* '237 IPR, Paper 15 (institution decision), 13, *with* '237 FWD 10–12. More importantly, Patent Owner does not allege or attempt to show that the '009 patent supports or requires such "intent" as part of the broadest reasonable construction of the term "interception of a DNS request." We cannot find support in the record for such a requirement.[4]

Based on the foregoing discussion, the record shows that the additional functionality urged by Patent Owner should not be imported into the term "interception of the DNS request." Moreover, Petitioner's construction is consistent with the plain meaning of the term as well as with the language of the claim and Specification. Accordingly, the broadest

[4] Although not part of the claim construction, a requestor may "intend" for the entered domain name in a request to reach the target device, but the DNS intercepts it to perform the look up.

reasonable construction of the term "interception of a DNS request" includes "receiving a DNS request pertaining to a first entity at another entity."

OBVIOUSNESS OVER BESER AND RFC 2401

A. *Level of Ordinary Skill in the Art*

Petitioner's expert, Dr. Tamassia, states that a person of ordinary skill in the art would have "a good working knowledge of networking protocols, including those employing security techniques, as well as cryptographic methods and computer systems that support these protocols and techniques." Ex. 1005 ¶ 110; *see* Pet. 8–9. Such a person would have gained this knowledge "either through several years of practical working experience or through education and training" or some combination of both. *Id.*

Patent Owner argues that "Petitioner proposes a lower level of skill, but Patent Owner's proposed level is the same level of skill that Petitioner and nearly a dozen other parties have consistently advocated in related litigation involving patents in the same family" as the '009 patent. Prelim. Resp. 23[5] (citing Ex. 2005, 4; Ex. 2004, 5). Patent Owner's expert, Dr. Monrose, states that "a person of ordinary skill in the art [at the relevant time] would have had a master's degree in computer science or computer engineering, as well as two years of experience in computer networking with some accompanying exposure to network security." Ex. 2016 ¶ 13. Dr. Monrose adds that his "view is consistent with VirnetX's view that a person of ordinary skill in the art requires a master's degree in computer science or

[5] Patent Owner does not appear to renew this argument in its Response. *See* PO Resp. 9–10 n.3.

computer engineering and approximately two years of experience in computer networking and computer security." *Id.*

We are persuaded that Patent Owner's description of the background of a person of ordinary skill in the art is not lower than or inconsistent with Petitioner's description. Instead, Patent Owner's definition requires a particular educational background, but appears to result in the same level of expertise as Petitioner's definition. For purposes of this Decision, based on the testimony of the parties' experts as well as our review of the '009 patent and the prior art involved in this proceeding, we conclude that a person of ordinary skill in the art would have a master's degree in computer science or computer engineering and approximately two years of experience in computer networking and computer security—or the equivalent, obtained through practical work experience and training.

B. *Tamassia Declaration*[6]

Petitioner supports the assertions in its Petition with a declaration by Dr. Roberto Tamassia. Ex. 1005. Patent Owner argues that the entirety of Dr. Tamassia's declaration should be given little or no weight because "he failed to consider, let alone opine on, how any of the claim features are disclosed in asserted references." PO Resp. 51.

Petitioner responds that Dr. Tamassia has "offered probative testimony on many of the factual inquiries underpinning an obvious analysis" that "can certainly 'assist the tier of fact to understand the evidence

[6] We address Patent Owner's Motion to Exclude (Paper 35) certain paragraphs of Exhibit 1005 in a separate section, below.

or determine a fact in issue.'" Reply 23 (citing Fed. R. Evid. 702). Petitioner adds that "no rule requires an expert to opine on the ultimate question of obviousness or on every potentially relevant fact at issue for his opinion to be admissible or entitled to weight." *Id.*

Patent Owner has not articulated a persuasive reason for giving Dr. Tamassia's declaration, as a whole, little or no weight in our analysis. We agree with Petitioner that experts are not required to opine on every relevant factual and legal issue in order to be accorded substantial weight. The cases Patent Owner relies on do not persuade us otherwise. For example, Patent Owner cites *Schumer v. Laboratory Computer Systems, Inc.*, 308 F.3d 1304, 1315 (Fed. Cir. 2002), for the proposition that "expert testimony 'must identify each claim element, state the witnesses' interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference.'" PO Resp. 52. Patent Owner's quotation, however, mischaracterizes *Schumer* by omitting introductory words necessary to the meaning of the quoted sentence. In its entirety, the quoted portion of *Schumer* states the following:

> *Typically, testimony concerning anticipation* must be testimony from one skilled in the art and must identify each claim element, state the witnesses' interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference. The testimony is insufficient if it is merely conclusory.

Schumer, 308 F.3d at 1315–16. The Federal Circuit then adds that it is not the task of the courts to "attempt to interpret confusing or general testimony to determine whether a case of invalidity has been made out" and "if the

testimony relates to prior invention and is from an interested party, as here, it must be corroborated." *Id.* So, instead of laying out a specific, required format for the content of all testimony regarding invalidity, as asserted by Patent Owner, this portion of *Schumer* confirms the unremarkable proposition that conclusory, overly general, confusing, and self-interested testimony should not be relied upon. *Id.*; *see also Koito Mfg. v. Turn-Key-Tech, LLC*, 381 F.3d 1142, 1152 (Fed. Cir. 2004) ("General and conclusory testimony, such as that provided by Dr. Kazmer in this case, does not suffice as substantial evidence of invalidity."). Patent Owner has not shown that the whole of Dr. Tamassia's testimony suffers from any of these failings.

Under 37 C.F.R. § 42.1(d), we apply the preponderance of the evidence standard in determining whether Petitioner has established unpatentability. In doing so, it is within our discretion to determine the appropriate weight to be accorded the evidence presented, including expert opinion, based on the disclosure of the underlying facts or data upon which that opinion is based. Thus, we decline to make a determination about Dr. Tamassia's opinion, as a whole. Rather, in our analysis we will consider, as it arises, relevant portions of Dr. Tamassia's testimony and determine the appropriate weight to accord that particular testimony.

C. *Prior Art Printed Publication Status of RFC 2401*

Patent Owner asserts that Petitioner has not sufficiently established that RFC 2401 qualifies as a printed publication as of its alleged publication date. PO Resp. 42–43. We look to the underlying facts to make a legal determination as to whether a document is a printed publication. *Suffolk*

Techs., LLC v. AOL Inc., 752 F.3d 1358, 1364 (Fed. Cir. 2014). The determination of whether a document is a "printed publication" under 35 U.S.C. § 102(b) involves a case-by-case inquiry into the facts and circumstances surrounding its disclosure to members of the public. *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). Public accessibility is a key question in determining whether a document is a printed publication and is determined on a case-by-case basis. *Suffolk Techs.*, 752 F.3d at 1364. To qualify as a printed publication, a document "must have been sufficiently accessible to the public interested in the art." *In re Lister*, 583 F.3d 1307, 1311 (Fed. Cir. 2009).

In our Decision to Institute, we found that RFC 2401 included indicia suggesting a reasonable likelihood that the document was made public because (1) RFC 2401 is a dated "Request for Comments" from the "Network Working Group," discussing a particular standardized security protocol for the Internet, and (2) it describes itself as a "document [that] specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. . . . Distribution of this memo is unlimited." Inst. Dec. 7 (citing Ex 1008, 1). On this basis, we determined that Petitioner had met its burden for a threshold showing to proceed to trial. *Id.*

In support of Petitioner's position, Dr. Tamassia testifies that RFCs are "prepared and distributed under a formalized publication process overseen by one of several Internet standards or governing bodies," such as the IETF. Ex. 1005 ¶ 148. Dr. Tamassia goes on to discuss an RFC that discusses the RFC development and publication process itself—RFC 2026,

dated October 1996. *Id.* at ¶¶ 149–55; Ex. 1036. Dr. Tamassia states that "[t]he publication date of each RFC is contained in the RFC, typically in the top right corner of the first page of the document" and "[t]his is the date it was released for public distribution on the Internet." *Id.* at ¶ 152. RFC 2026 also explains that anyone can obtain RFCs from a number of Internet hosts and each RFC "is made available for review via world-wide on-line directories." Ex. 1036, 4; *see* Ex. 1005 ¶¶ 148–49.

Patent Owner argues that Petitioner cannot rely on evidence it has proffered to support this finding. First, Patent Owner argues that testimony by Dr. Tamassia should not be accorded any weight because Dr. Tamassia has not been established to have personal knowledge that RFC 2401 was actually released to the public in November 1998 nor has Dr. Tamassia "been established as someone familiar with, let alone an expert in, the workings of the internet Engineering Task Force (IETF)—the body responsible for the RFCs." PO Resp. 44–45.[7]

We find Dr. Tamassia's testimony as to public accessibility of RFCs in general to be credible, especially given the independent support of RFC 2026 (Ex. 1036), the contents of which Patent Owner does not challenge. As part of routine discovery (37 C.F.R. § 42.51(b)(1)(ii)), Patent Owner had

[7] Patent Owner also argues we should give Dr. Tamassia's testimony on this issue no weight because the Petition does not cite to these paragraphs. PO Resp. 44 n.5. Patent Owner, itself, however, directed the Board's attention to this testimony in its Preliminary Response (Paper 6, 3–4), and, thus, clearly has had adequate notice of its contents such that it may respond with no resulting prejudice.

the opportunity to cross-examine Dr. Tamassia, but does not point us to any discussion of this issue. Moreover, RFC 2401's contents are consistent with the publication process described by RFC 2026 and Dr. Tamassia, including the inclusion of a date "November 1998" on the top right corner of the first page of the document. In addition, this document—a request for suggestions and improvements for an Internet standards protocol, having no indication of being a mere draft or internal paper—is precisely the type of document whose very purpose is public disclosure.

"A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.* 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)). We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401(dated November 1998) was sufficiently disseminated to persons of ordinary skill interested in computer networking and security to be deemed "publicly accessible" at the relevant time. Therefore, on this record, we determine RFC 2401 qualifies as a prior art printed publication under 35 U.S.C. § 102(b).

D. *Beser Disclosure*

Beser describes a system that establishes an IP (internet protocol) tunneling association on a public network between two end devices. *See* Ex. 1007, Abs. Figure 1 of Beser is reproduced below.

FIG. 1

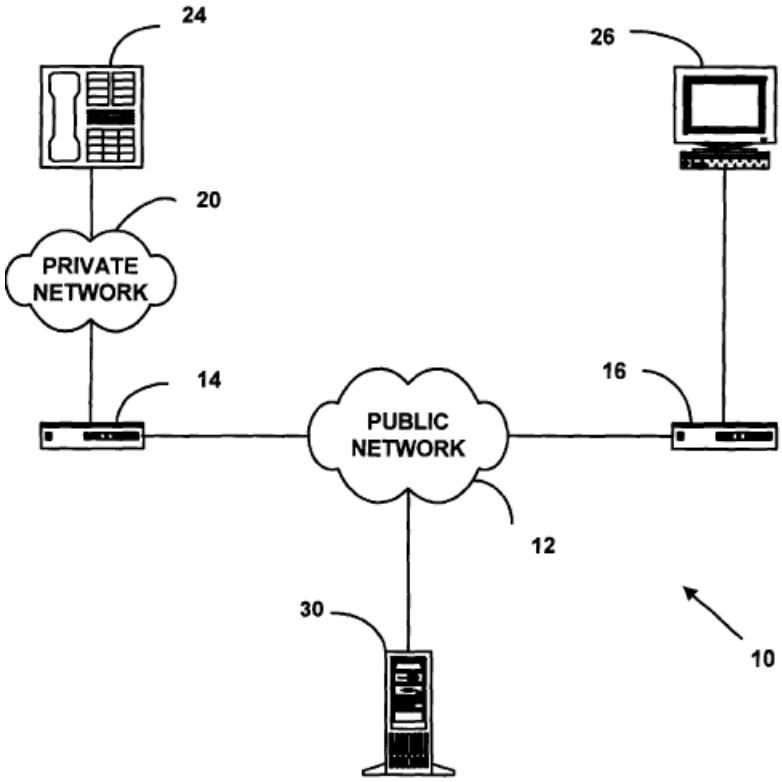

Figure 1 of Beser illustrates a network system, including public network 12, network devices 24 and 26, private network 20, trusted third-party network device 30, and modified routers or gateways 14 and 16. Ex. 1007, 3:60–4:19. Beser describes edge routers, such as network devices 14 and 16, as devices that route packets between public networks 12 and private networks 20. *Id*. at 4:18–24. End devices 24 and 26 include network multimedia devices, VoIP devices, or personal computers. *Id*. at 4:43–54.

Beser's system "increases the security of communication on the data network" by providing and hiding, in packets, "private addresses" for

originating device 24 and terminating device 26 on the network. *See id.* at Abs., Fig. 1, Fig. 6. To begin a secure transaction, requesting device 24 sends a request to initiate a tunneling connection to network device 14. *Id.* at 8:21–47. This request includes a unique identifier for the terminating end of the tunneling association—terminating device 26. *Id.*at 7:64–8:3. The packets used to transfer this unique identifier across the public network "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network." *Id.* at 11:22–25. Beser discloses, as background prior art, known forms of encryption for the information inside these packets, including IP Security ("'IPsec'"). *Id.* at 1:54–56. Once network device 14 receives the request, it passes the request on to trusted-third-party network device 30. *Id.* at 8:3–4, 8:48–9:5.

Trusted-third-party network device 30 contains a directory of users, such as a DNS, which retains a list of public IP addresses associated at least with second network device 16 and terminating device 26. *See id.* at 11:32–58. DNS 30 associates terminating network device 26, based on its unique identifier (e.g., domain name, or other identifier) in the request, with a public IP address for router device 16 (i.e., the association of the domain name with other stored information, including Internet addresses, shows they are connected together at the edge of public network 12). *See* Ex. 1007, 11:26–36, Figs. 1, 4, 5.[8] As indicated, DNS 30 includes, in a directory database or

[8] Figure 5, which includes step 116, involves a specific Voice-over-Internet-Protocol (VoIP) application of the general process of Figure 4, which includes parallel step 106. *See* Ex. 1007, 3:26–30.

otherwise, stored public IP addresses for router 16 and terminal device 26, and other data that associates devices 16 and 26 together. *Id*. at 11:48–52. In other words, trusted-third-party network device DNS 30, includes the "IP 58 addresses for the terminating . . . device[s] 26," and uses "data structures . . . known to those skilled in the art . . . for the association of the unique identifiers [for terminating devices 26] and IP 58 addresses for the . . . network devices 16"—including domain names as unique identifiers, as noted above. *Id*. at 11: 2–5, 32–36, 48–55.

Trusted-third-party network device 30 then assigns, by negotiation, private IP addresses to requesting network device 24 and terminating device 26. *Id.* at 9:29–35, 12:17–19, Figs. 4, 5. In an exemplary embodiment, trusted-third-party network (DNS) device 30 performs the negotiation for private addresses in order to further ensure anonymity of end devices 24 and 26 (though device 30 need not be involved in the negotiation in one embodiment). *Id*. at 9:29–35, 12:17–19. The negotiated private IP addresses are "isolated from a public network such as the Internet," and "are not globally routable." *Id*. at 11:63–65. "These IP 58 addresses may be stored in network address tables on the respective network devices, and may be associated with physical or local network addresses for the respective ends of the VoIP [(Voice-over- Internet-Protocol)] association by methods known to those skilled in the art." *Id*. at 12:33–37.

The negotiated private IP addresses may be "inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12." *Id*. at 12:15–16. The IP packets "may require encryption or authentication to ensure that the unique identifier cannot be read on the

public network 12." *Id.* at 11:22–25; *see also id.* at 20:11–14 (disclosing encryption or authentication of first IP 58 packet to ensure hiding the address of the public IP address of network device 16). Beser also discloses, as background prior art, known forms of encryption for "the information inside the IP packets," including IPsec. *Id*. at 1:54–56.

E. *RFC 2401 Disclosure*

RFC 2401 describes the security services offered by the IPsec protocols, including "access control, connectionless integrity, data origin authentication, [and] . . . confidentiality (encryption)." Ex. 1008, 3–4. RFC 2401 describes IPsec further, as follows:

> IPsec allows the user (or system administrator) to control the granularity at which a security service is offered. For example, one can create a single encrypted tunnel to carry all the traffic between two security gateways or a separate encrypted tunnel can be created for each TCP connection between each pair of hosts communicating across these gateways.

Id. at 7. The "security services use shared secret values (cryptographic keys) . . . . (The keys are used for authentication/integrity and encryption services)." *Id*.

F. *Claims 1 and 14*

Petitioner contends that the subject matter of independent claims 1 and 14 of the '009 patent would have been obvious over the combination of Beser and RFC 2401. Pet. 28–50; Reply 2–18. Petitioner supports its arguments with Declaration testimony of Dr. Tamassia. Ex. 1005. Although claim 1 recites "a network device" and claim 14 recites a "method executed by a first network device for communicating with a second network device,"

the two claims encompass substantially the same subject matter. Both Petitioner and Patent Owner argue claims 1 and 14 together. Pet. 28–50; PO Resp. 27–41; Reply 2–18. We, therefore, analyze the two independent claims together.

1. Petitioner's Assertions

Petitioner asserts that the "non-encrypted streaming audio/video example" described in Beser teaches each of the limitations of claims 1 and 14 except the required "encrypted communications link." Pet. 28–29, 34–50; Ex. 1005 ¶¶ 36–40, 74, 86, 91, 92, 94–96, 101, 278, 280–82, 286—93, 299, 300, 310, 316–20, 322–25, 327, 328, 330, 335–45, 358–60, 384–86, 401–403. Specifically, Petitioner argues that Beser's originating end device is equivalent to the claimed network device and Beser's terminating end device is equivalent to the claimed second network device. Pet. 34–35; Ex. 1005 ¶¶ 274, 278, 316, 320, 324, 335–40, 342–45.

Petitioner also argues that Beser discloses the trusted-third-party network device, intercepting a DNS request and determining that the terminating end device is available. Pet. 37–44; Ex. 1005 ¶¶ 86, 94–96, 299–300, 310, 317, 322–25, 327, 328, 330. If such determination is made, the trusted-third party device sends to the originating end device the private IP addresses of both the originating and terminating end devices that have been negotiated. Pet. 41–42 (citing Ex. 1007, 21:48–62). Petitioner equates the receipt of both IP addresses as the claimed "indication that the second network is available" and the receipt of the terminating end device's private IP address as the claimed "requested network address of the second network

address." *Id.* Petitioner concedes that "Beser would not provide provisioning information for an encrypted communication link," but that providing such information "would have been an obvious variation of Beser in view of RFC 2401" based on RFC 2401's description of encryption key distribution techniques. *Id.* at 42–44.

Finally, Petitioner equates the establishment of a virtual tunneling association between the originating end and terminating end of the tunneling association as the claimed communication link. Pet. 45–46. Petitioner concedes that "the *Beser* streaming video or audio example does not necessarily encrypt all the IP traffic sent over the secure tunnel," but asserts that encrypting all IP traffic being sent over the tunnel using end-to-end encryption would have been obvious considering the teachings of RFC 2401. *Id.* at 28–29, 45–46; Ex. 1005 ¶¶ 282, 283, 285, 383–90, 393, 394, 398–403.

Specifically, Petitioner argues that "a person of ordinary skill would have considered the teachings of Beser in conjunction with those in RFC 2401 because Beser expressly refers to the IPsec protocol (which is defined in RFC 2401) as being the conventional way that the IP tunnels described in Beser are established." Pet. 30 (citing Ex. 1007, 1:54–56; Ex. 1005 ¶¶ 383–85, 395). Petitioner adds that Beser also indicates that "its IP tunneling schemes are compliant with standards-based processes and techniques (e.g., IPsec), and can be implemented using pre-existing equipment and systems" and that "IP tunnels are and should ordinarily be encrypted." *Id.* at 30–31 (citing Ex. 1007, 1:54–56, 4:55–5:2, 11:22–25, 18:2–5; Ex. 1005 ¶¶ 185, 282–83, 383–86, 389–90, 394, 398). In addition, Petitioner contends that a person of ordinary skill would have recognized that IPsec readily could be

integrated into Beser's systems. *Id.* at 31–32 (citing Ex. 1005 ¶¶ 391, 392, 398–400).

2. Our Findings

We agree with Petitioner's analysis, summarized above, which we adopt, and determine that Petitioner has shown, by a preponderance of the evidence that Beser discloses all the limitations of independent claims 1 and 14 except the required communications link with end-to-end encryption and providing the related provision information for such link, both of which would have been an obvious variation of Beser's system based on the teachings of RFC 2401. We have reviewed both parties' arguments and supporting evidence, including the disclosure of both references and the testimony of Dr. Tamassia and Dr. Monrose. Pet. 28–29, 34–50; PO Resp. 23–42; Reply 3–18; Ex. 1005; Ex. 2016. For the reasons discussed below, we are not persuaded by Patent Owner's arguments to the contrary.

3. "Send[ing] a Domain Name Service (DNS) Request to Look up a Network Address of a Second Network Device Based on an Identifier Associated with the Second Network Device"

Petitioner relies on Beser's description of an originating end device requesting to initiate a tunneling association with a terminating end device for disclosure of this limitation. Pet. 35–36 (citing Ex. 1007, 7:64–8:1, 9:64–10:41; Ex. 1005 ¶ 316). According to Petitioner, this request contains a unique identifier, which can be a domain name, associated with the terminating end device. *Id.* at 36 (citing Ex. 1007 4:9–11, 8:1–3, 10:37–42, 10:37–11:8; Ex. 1005 ¶¶ 318–19); Reply 9. And the trusted-third party network device that processes this request can be a domain name server,

which looks up the public IP address associated with the domain name and negotiates private IP addresses for the originating and terminating end devices. *Id.* (citing Ex. 1007, 11:26–36, 11:45–58, 12:28–32, 17:42–49; Ex. 1005 ¶¶ 323–25); Reply 9. Thus, Petitioner concludes that Beser's tunneling request is a request for a resource corresponding to a domain name—a DNS request. *Id.* at 37; Reply 9.

Patent Owner argues that Beser's tunneling request is *not* a DNS request to look up a network address. PO Resp. 27–28 (citing Ex. 2016 ¶ 38). According to Patent Owner, there is no evidence that Beser's tunneling request follows the DNS protocol and "while tunneling requests may be received by a domain name server . . . *Beser* is silent as to whether tunneling requests 'follow the DNS protocol.'" *Id.* at 28 (citing Ex. 2016 ¶ 40). Patent Owner adds that the trusted-third party network does not look up any IP address, but rather the originating and terminating end devices negotiate private IP addresses and *assign* them to the devices. *Id.* at 29 (citing Ex. 1007, 8:9–15, 11:58, 12:2–4, Fig. 6 (step 118); Ex. 2016 ¶ 41). Moreover, Patent Owner argues that although Beser "states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26 . . . Beser never suggests that this data structure is looked up when the tunnel request is received by device 30, let alone that the public address of telephony device 26 is specifically looked up." *Id.* (citing Ex. 1007 11:26–32; Ex. 2016 ¶ 42).

Petitioner responds that nothing in the construction of "DNS request" requires the request to follow the DNS protocol. Reply 10. Moreover, according to Petitioner, Beser *does* teach that the tunneling request follows

the DNS protocol because a person of ordinary skill at the relevant time would have understood the functionality of a DNS server to use the DNS protocol. *Id.* (citing Ex. 1007, 1:50–53, 4:9–11; Ex. 1005 ¶¶ 303, 306, 307, 319, 327, 328). Petitioner contends that Beser discloses using the database of the trusted-third-party device 30 to "associate a public IP address for a second network device," after receiving the tunneling request, which is equivalent to looking up an IP address. *Id.* at 11 (citing Ex. 1007 11:26–54, Fig. 5).[9]

We agree with Petitioner's analysis and determine that Petitioner has shown, by a preponderance of the evidence, that Beser's tunneling request discloses the claimed DNS request and lookup of a network address of a second network device based on an identifier associated with the second network device.

First, we agree with Petitioner's analysis that Beser discloses a DNS request. Patent Owner explicitly agreed that the construction of "DNS request" was "a request for a resource corresponding to a domain name." PO Resp. 24; Tr. 47:20–51:10. And Beser discloses that (1) the tunneling request is a request for a resource; (2) the tunneling request includes "a

[9] Petitioner also points out that this particular limitation does not actually require a specific lookup be done, it just requires that the DNS request be sent. *Id.* at 10–11. Although this may be true, for purposes of this analysis we will assume that the claims require an actual lookup because, even if not required by this limitation, such a lookup is arguably required by the limitation "following interception of the DNS request and a determination that the second network device is available for a secure communications service," which is recited by both claims 1 and 14.

unique identifier for the terminating end [26] of the tunneling association" (*id*. at 8:1–3), which may be "a domain name" (*id*. at 10:37–41, 11:20–22); and (3) the trusted-third-party network device may act as a DNS server in some embodiments (*id*. at 4:9–11). We conclude that a preponderance of the evidence shows that Beser's tunneling request discloses a request for a resource (the network address of the terminating end device) corresponding to a domain name (the unique identifier for the terminating end device).

We are not persuaded by Patent Owner's argument that because Beser does not explicitly discuss using the DNS protocol, it does not disclose a DNS request. We credit Dr. Tamassia's testimony that, at the relevant time, DNS servers were conventional and DNS functionality was well-known. Ex. 1005 ¶¶ 303–07. Thus, a person of ordinary skill would have understood Beser's trusted-third-party device, acting as a DNS server, itself discloses any implicit requirement for a DNS protocol included in the term DNS request. And although Dr. Monrose states that "Beser is silent as to whether tunneling requests 'follow the DNS protocol'" (Ex. 2015 ¶ 39), Patent Owner points to no evidence contradicting Dr. Tamassia's testimony that a person of ordinary skill in the art would have been well-aware of the details of DNS functionality at the relevant time (*id.* at ¶¶ 38–43) or that the description of a DNS server implies the use of the DNS protocol.

Second, we agree that Beser discloses an actual lookup of the terminating end device's network address. Both Beser and the '009 patent itself disclose that a DNS server performs a lookup. For example, Beser states that "an appropriate Domain Name Server ('DNS') inquiry may correlate the IP address with a domain name, and domain names are

typically descriptive of the user, location, or the user's organization." Ex. 1007, 1:50–53; *see also id.* at 10:55–57 ("Other possibilities are that the unique identifier . . . is a domain name . . . used to initiate the VoIP association."), 10:37–41 (similar). Similarly, according to the '009 patent, "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host." Ex. 1003, 40:7–13. In addition, according to this conventional scheme, "[w]hen a user enters the name of a destination host, a request DNS REQ is made . . . to look up the IP address associated with the name." *Id*. at 39:19–23.

In addition, Beser discloses that, pursuant to the tunneling request, trusted-third-party device 30, with devices 14 and 16, or device 30 by itself, negotiates and looks up a private internet address for end device 26, in part by looking up a public internet address for device 16 based on the domain name associated with end device 26. *See* Ex. 1007, 10:37–57, 11:1–52, 12:6–19, 13:30–33; Reply 13 (citing Ex. 1007, 9:29–30, 12:16–19, 14:19–27, Figs. 6 and 9). As discussed above, Beser discloses that trusted-third-party device 30, acting as a DNS, may include a "database entry . . . includ[ing] a public IP 58 address[] *for the terminating telephony device 26*. Many data structures that are known to those skilled in the art are possible *for the association of the unique identifiers and IP 58 addresses for the second network devices 16*." Ex. 1007, 11:50–55 (emphases added). Therefore, in this disclosed embodiment, Beser's DNS 30 implicitly looks up the public IP 58 addresses of devices 16 and 26 based on a domain name (unique identifier) of terminating device 26—in order to associate the two devices.

Furthermore, based on the request packets, "[a] public network address for a second network device [16] is associated with the unique identifier on the trusted-third-party network device at Step 106." *Id*. at 8:4–7. In other words, "the second network device" 16 and its public address are "associated with . . . terminating end [26] of the tunneling association" via the terminating end's "unique identifier" (a domain name), and/or any number of "database entr[ies]," which provide an association, including "public IP 58 addresses for the terminating . . . device 26." *See id*. at 8:4–9, 11:45–55. After this association between device 16 and 26, in step 108, "the second private network address is assigned to the terminating end [26] of the tunneling association." *Id*. at 8:13–15, Fig. 4.

The record shows that at least a domain name for terminating end device 26 (i.e., "the second device" of claims 1 and 14) in the request packet constitutes a request, intercepted by trusted-third-party device 30—acting as a DNS server ("DNS 30")—and device 14, to look up the network address of terminating end device 26. In addition to an implied look up (i.e., an association) of the public IP address of device 26 by DNS 30, Beser's network device 16 looks up the private IP address of device 26—after DNS 30 and network device 14 receive the request for a look up. *See, e.g.*, Ex. 1007, 13:49–64, 16:1–37; Pet. 23, 41; Reply 13–14.

In summary, Beser discloses looking up the private and public IP addresses for terminating end device 26. Ex. 1007, 11:50–55. To make the association, Beser's DNS 30, a directory service, stores public IP addresses for device 26 under one option. Ex. 1007, 11:45–55; *see also* Inst. Dec. 9 ("Trusted-third-party network device 30 contains a directory of users, such

as a DNS, which retains a list of public IP addresses associated at least with second network device 16 and terminating devices 26.") (citing Ex. 1007, 11:32–58); PO Resp. 29 ("*Beser* . . . states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26.) (citing Ex. 1007, 11:50–55). Therefore, Beser implies that it associates devices 16 and 26 by, among other ways, looking up the public IP addresses of both of those devices as stored in a DNS database, based on the unique domain name for device 26. Ex. 1007, 11:45–55. Patent Owner does not dispute that Beser's system, including DNS 30, associates the public IP addresses of 16 and 26 with the domain name of device 26 and returns a private IP address for terminating device 26. *See* PO Resp. 31–32.

We, therefore, conclude that Petitioner shows by a preponderance of evidence that Beser discloses sending the claimed DNS request to look up the network address of a second network device based on an identifier associated with the second network device.

4. "Interception of the DNS Request"

Petitioner relies on Beser's description of the functionality of both the first network device 14 and the trusted-third-party network device 30 for disclosure of "interception of the DNS Request." Pet. 37–38; Tr. 6:23–7:11. First, the first network device intercepts the request sent by the originating end device with a unique identifier associated with the terminating end device. Pet. 37–38 (citing Ex. 1007, 8:21–47; Ex. 1005 ¶¶ 86, 299–300). Second, if the first network device determines that the request is to initiate

an IP tunnel, it is forwarded to the trusted-third-party network for special processing. *Id.* at 37–38 (citing Ex. 1007, 8:21–47; Ex. 1005 ¶ 322). As construed above, the term "interception of a DNS request" means "receiving a DNS request pertaining to a first entity at another entity." According to Petitioner, the first network device and the trusted-third-party device receive a request pertaining to the terminating end device. *Id.*

Patent Owner responds that the tunneling request cannot be "intercepted" by first network device 14 or trusted-third-party network device 30, because in Beser's system, tunneling requests "always go to, and are always intended to go to the first network device." PO Resp. 32. Patent Owner contends that Petitioner's expert, Dr. Tamassia, required an element of intent in the construction of "interception of a DNS request" and Beser does not satisfy the requirement. *Id*. at 32–33 (citing Ex. 2016 ¶ 44; Ex. 2015, 80:3–13).

Patent Owner's contentions are not persuasive. As set forth above, the "interception of a DNS request" does not include an element of intent. Furthermore, no party proposed an "intent" element in the construction of the "interception" limitation in this proceeding. Reply 15; PO Resp. 4 (listing both parties' claim construction proposals).[10]

[10] Accordingly, it is not necessary to reach Petitioner's explanation that Beser's originating device 24 "intends for" packets with look up requests to go to first device 14, and that trusted-third-party device 30 "intercepts" those packets. *See* Reply 15–16.

In any event, as Petitioner explains, regardless of what any potential "intent" element of "interception of a DNS request" entails, in Patent Owner's disclosed system, all requests are intended to go to the proxy DNS (i.e., not another entity), which the Specification characterizes as "intercept[ing] all DNS lookup functions" (Ex. 1003, 40:39–41):

> The only disclosure in the '009 patent of a DNS device that "intercepts" lookup requests is DNS proxy 2610, which "intercepts *all DNS lookup functions* from client 2605." Ex. 1003 at 40:39–41 (emphasis added). The '009 patent thus provides that DNS proxy 2610 "intercepts" lookup functions, even though the DNS proxy receives every single lookup request sent by the client. *Id*. at Fig. 26, 40:39–41. Dr. Monrose agreed that the DNS proxy in the '009 patent receives every DNS request and that the system is designed, *i.e.*, "pre-established" to intercept every DNS request. Ex. 1066 at 55:8–20. Thus, the Board should reject Patent Owner's arguments that Beser cannot show an "interception" because the system is designed such that IP tunnel requests are received by network device 14 and trusted device 30.

Reply 15.

Dr. Monrose agreed during his deposition to Petitioner's characterization that the '009 patent's disclosed proxy DNS is "designed to intercept all DNS lookup functions." Ex. 1066, 55:8–20. Therefore, the record shows that Beser's first network device 14 and trusted-third-party device 30 operate just like the disclosed proxy DNS in the context of intercepting requests. In other words, as explained above in the claim construction section, the '009 patent treats "intercepting" by the intermediate proxy DNS as "receiving" a request to look up an address for another entity (e.g., a target or end

device), and both parties agree "receiving" constitutes "intercepting." *See*, Tr. 31:8–23 (Patent Owner counsel stating that the related '705 patent does not specify how interception occurs), 37:12–21 (Patent Owner counsel stating that if we adopted Patent Owner's construction of "interception of DNS request," Beser does not pose a patentability problem because it does not disclose encryption—not because it does not receive the DNS request.).

5. The Receiving Limitation

Patent Owner argues that Petitioner improperly relies on two elements in Beser for three separate claimed features. PO Resp. 40–42. Specifically, claims 1 and 14 recite a first network device

> receiv[e/ing], following interception of the DNS request and a determination that the second network device is available for a secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link.

("the receiving limitation"). According to Patent Owner, Petitioner improperly contends that the first two enumerated features of the receiving limitation—the indication and the requested network address—are satisfied by Beser's receipt, at the originating end device, of only one element—the private IP address of the terminating end device. *Id.* at 40–41 (citing Pet. 41–42). Patent Owner adds that "Petitioner has not argued that one of skill would have found it obvious to either replace the three separate claim features with two features that perform multiple functions or add an

additional element to Beser to be received by the originating device." *Id.* at 42.[11]

We do not agree with Patent Owner that Petitioner's arguments are so limited. In fact, the Petition asserts that after a tunneling request, the originating end device receives both (1) the private IP address of the terminating device 26, and (2) its own private IP address. Pet. 41–42 (citing Ex. 1007, 21:48–62); *see also* PO Resp. 42 (quoting Ex. 1007, 21:48–52). Moreover, Beser's description of the private IP address of terminating device 26 clearly equates to the claimed "requested network address of the second network device." According to Petitioner, the originating network device, also receives an "indication," because it "receives a second private IP address: its own." Reply 17–18 (citing Pet. 41); *see also* Ex. 1005 ¶ 341 ("Receipt of the two private IP addresses would be an indication to the originating end device that the trusted-third-party network device has established an IP tunnel."). We agree that Beser's description of the originating network device receiving both its own private IP address and that of the terminating end device qualifies as the claimed "indication that the second network device is available for the secure communications service." Ex. 1007, 21:48–62; Ex. 1005 ¶¶ 333–45.

[11] Patent Owner does not address, in its Response, the third enumerated feature of the receiving limitation. As discussed above, a preponderance of the evidence supports a finding that providing such provisioning information would have been an obvious variation of Beser in view of RFC 2401. Ex. 1008, 6–7; Ex. 1005 ¶¶ 136–40, 358–60, 401–03.

Although it is true, as Patent Owner suggests, that Petitioner "relies on an overlapping disclosure of Beser to address" (PO Resp. 40–41) two of the recited pieces of information received by the originating end device, we are persuaded that a preponderance of the evidence supports a finding that a person of ordinary skill in the art would have found this limitation obvious notwithstanding that overlapping disclosure.

The case law Patent Owner relies on does not require a finding to the contrary. *See* PO Resp. 41–42. The elements at issue here are not structures (as opposed to the spring means and the hinged arm of *Becton, Dickenson & Co. v. Tyco Healthcare Group, LP,* 616 F.3d 1249, 1254 (Fed. Cir. 2010) or the two conveyors in *Lantech, Inc. v. Keip Mach. Co.*, 32 F.3d 542, 545 (Fed. Cir. 1994)) and do not recite performing functions (as opposed to the various fastening mechanisms of *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999)). Instead, the recited elements represent information received by one device from another device. There is no "clear implication" from the claim language that the two pieces of information cannot overlap. To the contrary, the specification suggests that the two elements are *not* completely independent by stating that the indication *includes* the requested network address of the second network device. Ex. 1003, 8:20–25 ("receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device"), 8:37–41. In light of this disclosure, we agree with Petitioner that a person of ordinary skill would find the claimed indication obvious based on Beser's teaching that the private IP address of both the originating end device and the terminating end device 26

is sent to the originating end device even though the second address also satisfies the second recited received piece of information. *See* Ex. 1007, 14:19–27, 14:57–62, 21:48–62; Ex. 1005 ¶¶ 340–41.

We, therefore, conclude that Petitioner shows by a preponderance of evidence that the receiving limitation would have been obvious in view of Beser and RFC 2401.

6. Combination of Beser and RFC 2401

As noted above, Petitioner provides several reasons explaining why an artisan of ordinary skill would have used end-to-end encryption, as disclosed and suggested by RFC 2401, in Beser's similar network system, for example, to provide enhanced data security and anonymity in networks having similar topology. Pet. 30–32. Petitioner also notes that Beser itself suggests the encryption of data using the IPsec protocol, the same encryption protocol that RFC 2401 defines. *See* Pet. 30–31; Ex. 1007, 1:54–56; Ex. 1008, 4. Petitioner contends that RFC 2401 provides automatic encryption for traffic traveling through security gateways over a public network, and that Beser employs edge routers and similar gateways, thereby at least suggesting encryption for a secure tunnel. *See* Pet. 31–32; Ex. 1008, 4–6, 30. RFC 2401 describes an IPsec goal as providing "confidentiality (encryption)." Ex. 1008, 4.

In response, Patent Owner argues that Beser and RFC 2401 would not have been combined as asserted by Petitioner. PO Resp. 33–40. Patent Owner contends that Beser teaches away from encryption. According to Patent Owner, Beser explains that prior art systems typically addressed

Internet security either by encrypting the information inside packets prior to transmission or by using address translation. PO Resp. 34 (citing Ex. 1007, 1:53–2:35). Beser acknowledges that both solutions have disadvantages, for example, encryption can "require a great deal of computing power to encrypt or decrypt the IP packets on the fly." *Id.* (citing Ex. 1007, 1:62–63). Patent Owner contends that Beser notes the problems with allocating more computing power to encryption, such as "jitter, delay, or the loss of some packets," and, therefore, "dismisses the idea of encryption entirely, noting that the 'expense of added computer power might also dampen the customer's desire to invest in VoIP equipment' at all." *Id.* at 34–35 (citing Ex. 1007, 1:654–67).

Patent Owner also contends that Beser only "proposes a method of hiding the addresses of originating and terminating devices":

> By hiding the identities of the network devices in this manner, *Beser* touts that its method is able to *increase* communication security *without increasing* computational burden. ([Ex. 1007,] 2:43–3:14.) Thus, one of ordinary skill in the art would have understood that Be*ser* is directed to providing a method for securing communications *other than* encryption. (*See* Ex. 2016 at ¶ 52.)

PO Resp. 36.

Patent Owner explains that "*Beser* also teaches that encryption does not deter a determined hacker from deducing source and identity information, and so, once the tunnel is established, *Beser* eschews encryption in favor of hiding the identities within the tunnel." PO Resp. 37. According to Patent Owner, the purpose of the encryption in *Beser* "is simply to hide address information on the public network prior to *Beser's*

tunnel establishment, once the tunnel is created, the originating and terminating device information is hidden and encryption would not only be redundant, it would contravene *Beser's* express objective of increasing security without increasing computational burden." *Id*. at 37–38 (citing Ex. 2016 ¶ 54).

We do not agree with Patent Owner's description of what a person of ordinary skill would have understood from Beser's disclosure. Although Beser recognizes that the use of encryption may cause challenges, Beser also suggests that such problems may be overcome by providing more computer power and/or less quality. *See* Ex. 1007, 1:60–67. For example, Beser teaches that an "increased *strain on computer power* [i.e., as opposed to increased computer power] may result in jitter, delay, or the loss of some packets." *Id*. at 1:63–64. Moreover, Beser never states that its technique of hiding addresses is intended as replacing, as opposed to supplementing, known security techniques such as encryption. In fact, Beser implies that a good system will allow multiple types of security solutions to be used at the same time, by characterizing some prior art systems as creating "*security problems by preventing certain types of encryption from being used*." Ex. 1007, 2:23–24 (emphasis added).

We credit testimony by Dr. Tamassia stating that "[a] person of ordinary skill in the art reading *Beser* in February 2000 would also have understood that encryption should ordinarily be used even in high data volume applications, if possible" and that such a person "would recognize that the concerns expressed in *Beser* . . . can be easily resolved by simply using more powerful equipment." Ex. 1005 ¶¶ 389–90. Dr. Tamassia's

conclusion is supported by explanation and citation to the record. Ex. 1005 ¶¶ 384–399 (citing Ex. 1007, *passim*; Ex. 1008, 25). Dr. Monrose's testimony does not persuade us to the contrary as it largely echoes Patent Owner's unpersuasive attorney argument. *Compare* Ex. 2016 ¶¶ 47–55, *with* PO Resp. 33–40. We find that Beser at most mildly criticizes (tempered by an implied solution) a specific type of tunneling that employs encapsulation, encryption, and VoIP packets—i.e., "due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets." Ex. 1007, 2:15–17. In other words, Beser at least suggests that with adequate power or typical data transmissions, a tunnel (a VPN according to Beser) and encryption would be appropriate for providing security. Therefore, we find that Beser does not discourage encrypting data to make it secure; rather, Beser provides a solution for providing anonymity by using a tunnel technique with or without encryption of data, and if necessary, increasing computer power as needed.

Thus, notwithstanding Patent Owner's arguments, a preponderance of evidence supports a finding that a person of ordinary skill reading Beser at the relevant time would have understood that encryption should ordinarily be used to protect the contents of the communications in an IP tunnel. Petitioner, thus, establishes by a preponderance of the evidence that a person of ordinary skill would have found it obvious to combine the teachings of RFC 2401 with those of Beser to encrypt data in order to enhance data security in a tunnel that provides anonymity, based on a determination that a requested target device would have been available for a secure communication.

G. *Claims 2–8, 10–13, 15–20, and 22–25*

Petitioner asserts that the combination of Beser and RFC 2401 teaches each of the limitations of claims 2–8, 10–13, 15–20, and 22–25. Pet. 50–59. According to Petitioner, Beser discloses each of the limitations added to independent claims 1 and 14 by the challenged dependent claims 2–8, 10, 13, 15– 20, 22, and 25. *Id.* at 50–56, 59. For claim 11 and 23, Petitioner asserts that a person of ordinary skill in the art would have considered it obvious include end-to-end encryption to Beser based on the teachings in RFC 2401 and, thus, would have found obvious the additional limitation "wherein the encrypted communication link is an end-to-end link extending from the network device to the second network device." *Id.* at 56–57 (citing Ex. 1005 ¶ 399). For the limitation added by claims 12 and 24, "wherein the intercept[ion/ing] the DNS request consists of receiving the DNS request to determine that the second network device is available for the secure communications service," Petitioner asserts that it would have been an obvious engineering design choice to a person of ordinary skill in the art at the relevant time. *Id.* at 57–58 (citing Ex. 1005 ¶¶ 323–30). Thus, Petitioner concludes that a person of ordinary skill would have found the claimed subject matter in claims 2–8, 10–12, and 22–25 obvious in view of Beser combined with RFC 2401. *Id.* at 50–59.

In its Response, Patent Owner does not make specific arguments directed to the challenged dependent claims and instead argues that "*Beser* and RFC 2401 do not render obvious claims 2–8, 10–13, 15–20, and 22–25 for at least the reasons discussed above for independent claims 1 and 14, from which they depend." PO Resp. 42; *see also* Paper 9, 3 ("The patent

owner is cautioned that any arguments for patentability not raised in the response will be deemed waived.").

We have reviewed both parties' arguments and supporting evidence, including the disclosure of both references and the testimony of Dr. Tamassia and Dr. Monrose and we agree with Petitioner's analysis and adopt it as our own. Thus, we determine that Petitioner has shown, by a preponderance of the evidence, that a person of ordinary skill in the art would have found dependent claims 2–8, 10–13, 15–20, and 22–25 obvious over Beser and RFC 2401.

PATENT OWNER'S MOTION TO EXCLUDE

Patent Owner seeks to exclude Exhibits 1001, 1002, 1009–35, 1037–41, 1043–48, 1060, 1063–65, 1068, 1069, and portions of 1005. Paper 35, 1. As movant, Patent Owner has the burden of proof to establish that it is entitled to the requested relief. *See* 37 C.F.R. § 42.20(c). For the reasons stated below, Patent Owner's Motion to Exclude is *denied*.

1. Exhibits 1060 and 1063–65

Patent Owner seeks to exclude Exhibits 1060 and 1063–65 as inadmissible hearsay. Paper 35, 2. Exhibit 1060 is a declaration originally submitted in litigation before the International Trade Commission. Ex. 1060. It contains testimony from Sandy Ginoza, a representative of IETF, in support of Petitioner's contention that RFC 2401 qualifies as a printed publication as of November 1998. *Id.* Exhibit 1063 is a "transcript of Ms. Ginoza's February 8, 2013 deposition that was taken as part of the ITC action." Paper 35, 2 (quoting Paper 17, 5–6). Exhibits 1064 and 1065 are

both magazine articles dated 1999 that relate to the same issue. Paper 17, 5–7. All four exhibits were entered into the record upon Petitioner's Motion to Submit Supplemental Information Pursuant to 37 C.F.R. § 42.123(a). Paper 17; Paper 21.

Because we do not rely on any of these Exhibits to decide the issue of whether RFC 2401 qualifies as a printed publication, we dismiss the motion as to these Exhibits as moot.

2. Exhibits 1001, 1002, 1009–35, 1037–41, 1043–48, 1068, and 1069

Patent Owner seeks to exclude the above-listed exhibits as lacking relevance. Paper 35, 3. Because we do not rely on any of the exhibits listed above, , we dismiss this request as moot.

3. Portions of Exhibit 1005

Patent Owner seeks to exclude portions of Dr. Tamassia's testimony in Exhibit 1005 as lacking relevance. Paper 35, 4. Because we do not rely on any of the listed paragraphs of Exhibit 1005, we dismiss this request as moot.

ORDER

Accordingly, it is

ORDERED that claims 1–8, 10–20, and 22–25 of U.S. Patent No. 8,850,009 B2 are *unpatentable*;

FURTHER ORDERED that each Patent Owner's Motion to Exclude is *dismissed as moot*;

FURTHER ORDERED that, because this Decision is final, a party to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:
Jeffrey P. Kushan
Scott Border
Thomas A. Broughan, III
SIDLEY AUSTIN LLP
jkushan@sidley.com
sborder@sidley.com
tbroughan@sidley.com
iprnotices@sidley.com

PATENT OWNER:
Joseph E. Palys
Naveen Modi
Daniel Zeilberger
Chetan R. Bansal
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com
danielzeilberger@paulhastings.com
chetanbansal@paulhastings.com

Jason Stach
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
jason.stach@finnegan.com